Annual Security Refresher Briefing

NNSA Security Division Los Alamos

Annual Security Refresher Briefing

Welcome to the Annual Security Refresher Briefing for Los Alamos National Laboratory. This briefing includes information on general security, computer security, escorting, technical surveillance countermeasures, the hostile intelligence threat, and new security initiatives.

By completing this training, you will have satisfied the following training requirements:

- Annual Security Refresher-required for all active clearance holders.
- Annual Computer Security Refresher-required for all computer users.
- Technical Surveillance Countermeasures-required annually for all active employees at the Laboratory.

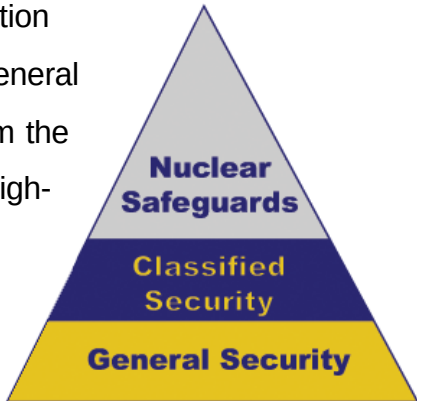
The purpose of this briefing is to make all lab workers aware of their individual security requirements: "Security is your responsibility!"

All employees holding a DOE clearance are REQUIRED to take the Annual Security Refresher every year. A notice will be sent to employees 60 days before, 10 days before, and the day of training expiration. If an employee's training expires, Personnel Security will be notified to take appropriate action up to, and including, making a recommendation to DOE/AL that the security clearance be terminated.

This year's briefing was developed using Integrated Safeguards and Security Management (ISSM) principles. Much of the briefing data came from feedback and improvement suggestions to the Security Help Desk. We developed this briefing to help you perform your work in a secure manner. We will collect your feedback and improvement suggestions on this briefing for incorporation into next year's briefing.

Annual Security Refresher Briefing

A major part of security at the lab is ISSM, Integrated Safeguards and Security Management. ISSM is a system for performing work securely, a way of doing business. ISSM provides a framework to support lab workers in fulfilling his/her security responsibilities so that we do not compromise the security of our nation as well as satisfy the security requirements that have been put forth by the US-DOE contract. ISSM works hand-in-hand with Lab LIRs (the Laboratory Implementation Requirements). LANL developed an integrated set of three security LIRs — General Security, Classified Security, and Nuclear Safeguards. These were derived from the I.S.S.M. Laboratory Performance Requirement (or LPR). The LPR provides a high-level description of ISSM, including the objective, guiding principles, and core functions for performing work securely. Together, the LIRs and LPR have been essential for achieving ISSM because they establish a common LANL-wide framework of security requirements for authorizing all LANL work.



Because security is all of our responsibility, there are many precautions you must take to ensure that the Laboratory remains secure. First, let's look at the personal electronic devices such as cell phones, two-way pagers and personal digital assistants, such as Palm Pilots.

Government-owned cell phones and two-way pagers may not be used in security areas or within fifty feet of a security area perimeter. A government-owned cell phone may be brought into a secured area if the battery is removed prior to entry and left out of the device while you are in a secured area. In special circumstances, permission to carry electronic communication devices in secure areas can be obtained from the LANL Communications Security Officer and the LASO Electronics Control Officer.

Annual Security Refresher Briefing

Personally owned cell phones are never allowed in secured areas, even with the battery removed. However, personal cell phones may be used in property protection areas and on Laboratory roads, parking lots, or other land that is routinely open to public access.

Privately owned personal digital assistants, or PDAs, are not allowed in any secured area. You may bring a government-owned PDA into a secured area as long as it does not have radio frequency, cellular transmission, or audio/video recording capabilities.

Palm pilots with infrared and/or serial ports, with or without expansion capabilities, must be addressed in an approved cyber security plan that lists applicable usage conditions and restrictions. Government-owned Palm pilots and other PDA's are never allowed for classified processing.

Another important security consideration is escorting people who do not have security clearances. It is important to be familiar with the policies that address escorting uncleared personnel and visitors.

The requirements for escorting uncleared US citizens in secure areas have recently changed. The most current procedures can be found on the Security Web site. You can also find the latest requirements for escorting foreign nationals on the Security Web site.

Annual Security Refresher Briefing

Security concerns are present in everyday tasks. You are responsible for security in everything you do in conjunction with your work. Your badge, the documents and media that you work with, the safes and vaults where information is kept, and the computer systems that you use all need to be kept secure at all times.

Protecting personal property such as your LANL badge is of utmost importance. Your badge identifies you as a Laboratory worker. It can tell an informed observer whether you are a DOE or contract employee, if you hold any type of clearance, and if you are in PSAP. It is very important wear your badge in view when on Laboratory owned or leased property. When your badge is not in use, ensure that you store it where it is safe from damage or theft. Loss or theft of a badge must be reported in person to the Badge Office within 24 hours OR the next business day.

Another security responsibility is to make sure all SAFES are secure to prevent any unnecessary security incidents. Safe owners and authorized workers are reminded to spin the dial during end-of-day checks. Regardless of the type of combination locking device, always check to make sure the repositories are securely locked.

Annual Security Refresher Briefing

Computer security precautions can be found in the Unclassified Cyber Security Plan. Every computer user is a link in the chain, all information has value, and sensitive information must not be disclosed, Always protect information from tampering. The Cyber Security Handbook is a valuable resource to refer to when you are working with Laboratory computers.

The cyber world at LANL is currently composed of three separate networks. The green network is open to the world. The yellow network is for unclassified sensitive information that is internal to the Lab, and the red is for classified processing. Currently, the Laboratory is developing two new networks; the visitor network, which contains Internet access only, and the Open Collaborative network, which is for wide-area projects.

The threats to cyber security can come from external sources, such as intruders from the outside who break into our system, or internal sources, who are insiders that, intentionally or not, disrupt the LANL computing environment.

Cyber security incidents disrupt cyber resources. These incidents include physical damage to resources, interfering with software or applications, introducing malicious code, unclassified system contamination, and unauthorized access. All potential cyber security incidents should be reported to your O.C.S.R., Organizational Computer Security Representative, commonly referred to as an OSCAR, or to the Cyber Security Team.

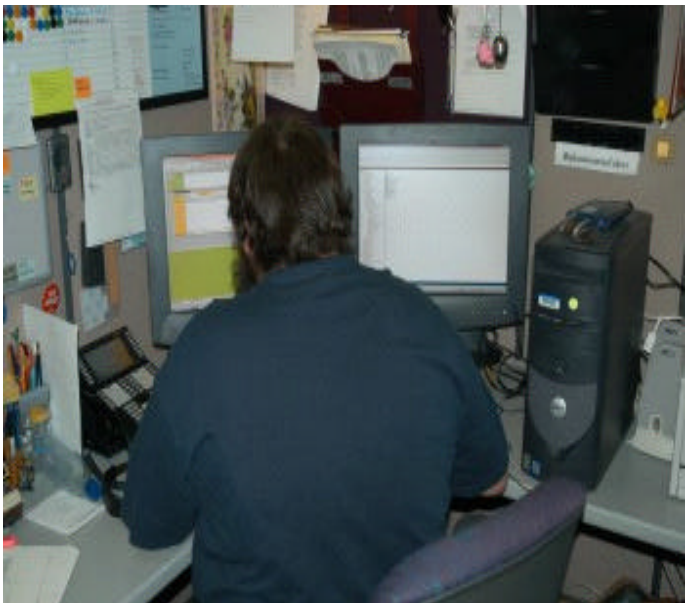
In order for foreign nationals to have computer access, some requirements must be met. The hosts of the foreign visitors and assignees must obtain pre-approval from management and the Foreign Visits and

Annual Security Refresher Briefing

Assignments Office. The Laboratory host must complete both Form 982, for general access, and Form 982CA for computer access. The security plan must document the risk assessment and identify access controls.

When using and installing software at or through the Laboratory, certain guidelines must be followed. Commercial software must be obtained through ESD or the regular procurement process. Software must have and abide by all licensing agreements. All software, including freeware and shareware, must be checked for viruses prior to installation, and all media used on a system must be approved.

Classified information cannot be processed on an unclassified system. If an unclassified system is contaminated by classified information, then the system must be unplugged from the network. The system must be protected and the incident needs to be reported immediately to your OCSR or to the Cyber Security Team.



Because computer technology is ever changing, new questions regarding cyber security come up all the time. Recently, a question has been raised about using wireless components in computer systems. The Lab's Cyber Security team has issued guidance on this issue. Wireless keyboards and mice are allowed in certain areas. Wireless Local Area Networks or LANs are prohibited in Limited and Exclusion Areas except in safety-related applications, and wireless LANs in open areas must be pre-approved. Contact your OCSR for details regarding wireless technology.

Annual Security Refresher Briefing

Ensuring cyber security at LANL is made up of many components. It is important to use your computer resources only for their intended work purposes. Always avoid non-work related activities and never use laboratory resources for pornography, gambling, hacking, etc. Choose passwords that follow DOE and LANL guidelines, and always protect them. The password guidelines can be found on the web. Back up all files and report any computer problems to your OCSR.

Protecting your work computer is a necessity. It's important to install virus protection and update it regularly. It is also important that your computer be protected while you are away from your desk or office. You can do this by enabling a password-protected screen saver, locking up sensitive media, using a boot-lock password, and locking your office.

Cyber security also plays a role if you are using a computer to work off-site. You should protect the resources at the same level as you would on-site systems. Property management procedures should be followed and if you are outside the United States, contact the SUP-2 Customs Office. If you are using non-LANL equipment on-site, it must be pre-approved and established guidelines and procedures must be followed.

When a computer changes ownership, follow the guidelines and procedures of the Property Management Manual and the Cyber Security Handbook. Equipment should never be transferred without property accountability. If you need assistance in marking and protecting media, or getting a system accredited for use, consult the Cyber Security Handbook.

Annual Security Refresher Briefing

Processing classified information has some serious risks. These include access by unauthorized users, breaches of security mechanisms such as passwords and firewalls, and disclosure or loss of information. It is your responsibility to protect the classified information you process at all times.

When it comes to accreditation, systems must not be used to process classified information until DOE has accredited that system. Before a system is accredited, a security plan must be approved. The system must be operated according to the security plan and significant changes to the system require re-accreditation of the system. Other concerns and questions should be directed to your OCSR or the Cyber Security Team.

We have discussed classified and non-classified systems, however, access to a classified system depends on two things: your clearance level, and your need-to-know. You must have both the proper clearance level and a need-to-know the information before access can be granted.

When saving files on a classified system, the classified media, such as diskettes, hard drives, etc, are accountable. All of the media must be marked and labeled, stored in an approved security container, and protected from unauthorized disclosure. For more information, consult the “Guidelines for Handling Classified Matter,” available on the Security Web site.

You must be very careful when deleting classified files, because deleting files does not completely destroy an electronic file. Please contact your OCSR, the Cyber Security Team (505-665-1795), or the Security Help Desk (505-665-2002) for assistance.

Annual Security Refresher Briefing

Computers and cyber resources are not the only things that need to be handled securely. Be aware of a photocopier that jams when copying sensitive and classified documents. If the machine jams, you should check all paper trays, the document glass, and the document feeder. Any and all jammed paper, unusable copies, and residue must be shredded in a shredder approved to destroy classified matter. Three blank pieces of paper must be run through the copier to clear the machine and the blank pages must then be shredded.

The Technical Surveillance Countermeasures, TSCM objective is to detect and/or deter a wide variety of technologies and techniques that can be used to obtain unauthorized access to classified and sensitive information.

The TSCM program is designed to ensure that all requirements, standards, and procedures contained in the DOE TSCM manual are followed. The program is not meant to be used in lieu of other security measures, but to enhance and reinforce existing security programs. TSCM Technicians assist in determining if adequate physical security construction and controls are in place.

The DOE TSCM program consists of four main points: detection, nullification, isolation, and education. Detection is used to find technical devices, security hazards, or physical security weaknesses that would permit the technical or physical penetration of sensitive/classified facilities. Nullification prevents, deters, and/or neutralizes technical devices that may be employed within a sensitive/security area. Isolation restricts sensitive and classified activities to special areas established by security authorities. Education of potential threats is vital to inform all personnel.

Annual Security Refresher Briefing

The TSCM program services include surveying, monitoring, inspecting, advising and assisting, awareness briefings (such as this training), and special services.

TSCM prohibits personal electronic devices containing recording, transmission, or wireless connectivity capabilities to be used in security areas where U.S. government protected information is processed or discussed. The national policy does not apply to those devices that only have the ability to receive commercial RF broadcasts or that only play prerecorded media.

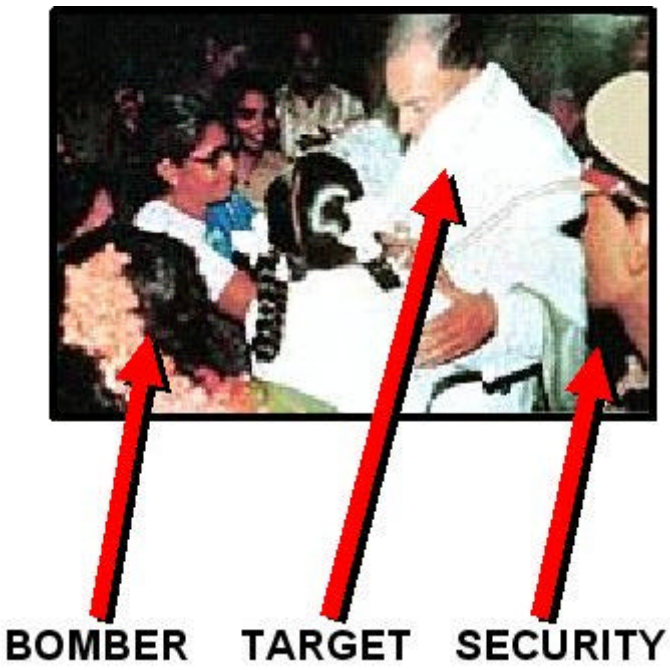
TSCM applies to everyone. Individuals must be aware of the nature of the technical threat and the part they play in the DOE Technical Surveillance Countermeasures Program. You should be aware that illegal surveillance devices may be used for purposes of collecting classified information, and you need to understand your responsibilities when you encounter this threat and how to report incidents if a technical attack occurs. If you discover a surveillance device, inform your line manager immediately.

In today's environment, the issue of hostile threats is a very real one. The threats can come from activists and from espionage. Always be aware of strangers in your work area. Do not answer questions about your work, access controls, co-workers, and other tenants, etc., until you have confirmed why the questions are being asked. All inquiries by journalists should be directed to the Public Affairs Office at (505) 667-7000. If you feel you are being targeted for information, contact your supervisor or the Security Help Desk at (505) 665-2002.

Annual Security Refresher Briefing

It is very important to note that there will always be adversaries from whom we must protect our vital secrets. That is why we practice Operations Security, otherwise known as OPSEC. This is a countermeasures program designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive departmental activities or information and to secure against inadvertent release of such information outside established control procedures.

Our individual responsibility is to protect information and resources. While it is important to learn and understand security, incidents can certainly turn risky and threatening. Now take a look at this picture. The person in the photograph is a suicide bomber. She was a Sri Lankan suicide bomber. This picture was taken moments before she killed former Indian Prime Minister Rajiv Gandhi, herself, and seventeen others. The bomb was concealed under her dress and smuggled through security at an election rally. She detonated the bomb while bending down to touch Gandhi's feet.



The threat of suicide bombers is increasing. The number of incidents during the 1980s and the 1990s increased. Many think that we are next. Vice President Dick Cheney states it's "inevitable." FBI Director Robert Mueller says it's "a real possibility."

Annual Security Refresher Briefing

Terrorist groups such as Al-Qu'ida could try to mimic Palestinian methods to cause panic here. There is no real suicide bomber characteristic. However, history has revealed that they are mostly male, 18–23 years old, and single. Nevertheless, bombers can be anybody and will often alter their appearance in order to blend in.

Suicide bombs can be delivered by multiple means such as

- vehicle bombs,
- boat bombs,
- individual-borne bombs,

all which can complicate security measures.

Terrorists will choose whichever method is most likely to succeed against a particular target, with the ultimate goal being to inflict as many casualties as possible. A suicide bomber's success depends on three major elements:

Secrecy, which is essential to plan and conduct the mission; thorough reconnaissance and surveillance, which is required to choose a target and identify its weakness; and extensive rehearsals and dry runs, which are necessary to ensure stealth and speed during the attack.

There is much we can do to prevent terrorist attacks and there are many things we need to remember. Traditional concepts of security assume the terrorist fears death or capture, but suicide attacks depend on the death of the terrorist. Remember that the suicide bomber doesn't care about his/her death, imprisonment or torture at the time of the attack, and that there is no need for an escape plan. Also take into account that the terrorist group wants to succeed, the suicide bomber does not want to die for nothing, and if a target is too tough, they will choose another.

Annual Security Refresher Briefing

There is no fool-proof method of preventing a determined bomber, however the surveillance/reconnaissance phase is the best time to stop attack planning, and it is important to be alert to indicators. The obvious ones are surveillance, particularly focusing on access points, dry runs to identify hazards or security checkpoints, and purchase of or illicit access to facility blueprints.

Some prevention tips are

- noticing unseasonable dress or conspicuous bulky clothes,
- obvious or awkward attempts to blend into a crowd,
- repeated or nervous handling of parts of clothing,
- profuse sweating,
- slow-paced walking while focusing on sides,
- attempts to stay away from security personnel,
- hesitant and nervous muttering,
- and heavily perfumed or recently shaved.

Currently, as a complement to the DOE security condition levels, the Laboratory defined several intermediate Security Condition levels (or SECONs) to facilitate a graded, flexible approach. Under the plan, different SECON options may be implemented. The current SECON level is posted on appropriate Laboratory web pages.

Based on vulnerability assessments and recommendations from DOE, two new traffic control stations will be constructed on Pajarito Road. The stations will be at the TA-3 and White Rock ends of the Pajarito corridor. These stations are still on the drawing board, and construction should be completed in the fall.

Annual Security Refresher Briefing

Even though everyone works hard to ensure that the Laboratory is kept safe and secure, incidents still happen. Incidents can occur when an employee unknowingly enters classified information into a machine or open email. Should a security incident occur in your organization, including the compromise, or potential compromise, of classified information, be aware that details of the incident itself are classified. Classified information about the incident includes any details such as the sender or source organization, recipients, date of the incident, and if it occurred over unclassified email or fax. Any information is classified if it could point an adversary to the information improperly released, such as the identification of a document or descriptions of its contents.

Remember, all inquiries from uncleared personnel regarding the information are subject to the DOE “no comment” policy.

Providing a secure workplace is essential to safety and security here at Los Alamos National Laboratory. We cannot succeed without your help and persistence in always following the provided guidance. Security is everyone’s responsibility.

To recieve credit for completing this breifing, click on the “Recieve Credit” button below or fill out the form on the following page and return it to the Security Registrar. Thank you and have a safe and secure day.

Recieve Credit

NNSA — Security Division — Los Alamos

Annual Security Refresher Briefing

Course Acknowledgment Form

By signing below, I certify I have read Los Alamos National Laboratory's Security & Safeguards 2003-2004 Refresher Briefing.

The contents of this course will be updated annually. If you print this course, for usage throughout the year, you are responsible for assuring you have the current version. Credit will not be provided if the current course content was not read. The last update was September 9, 2003. Please allow up to 5 working days before credit will appear in Employee Development System (EDS) database.

Z # _____

Name – printed _____

Signature _____

Date _____

Phone Number _____

Please fax to:
(505) 665-8984
Or mail to:
S-Division Registrar
PO Box 1663
Mail Stop K560
Los Alamos, NM 87545